Industrial Network Track: Multi-Bus

GarrettCom, Inc.
47823 Westinghouse Drive
Fremont, CA 94539
PH: (510) 438-9071
FAX: (510) 438-9072
www.GarrettCom.com

Industrial Network Track: Multi-Bus

Author Jim W. Hammond – Technical Consultant, GarrettCom, Inc.

Keywords: Network integration, Ethernet, TCP/IP, field buses, topology

Last time I checked it was reasonably easy to get a bus transfer in NYC, but don't expect that level of ease when doing transfers from one industrial bus to another. More than likely you'll get more attitude than a rush hour bus driver. What you need is a good map to avoid the roadblocks along the way, and a clear and logical itinerary that avoids the potholes. That is where this paper can help.

The interconnection and integration of existing heterogeneous sub-networks into a homogeneous network has always presented challenges. Evolving and converging protocol standards along with emerging multi-protocol components suggest that a clear understanding of the problems and solutions has never been more important. These concerns include reliability, redundancy, robustness, and security. Most importantly, the multi-bus points of integration should be as seamless as possible, and a consistently high level of security should be maintained throughout.

Where legacy equipment is still performing as required, an efficient way to integrate these components into the overall scheme while preserving security and reliability is vitally important. As new equipment and processes evolve, a consistent strategy of deployment of Ethernet-supported interfaces insures proper integration with a minimum of downtime and re-engineering delays. The wide range and availability of Ethernet solutions and its support from standards groups, vendors, OEMs, and industry provides the assurance that it will continue to evolve. From the early days of 10Mb coaxial cable products Ethernet has moved into the gigabit range and beyond. Bandwidth and media support outstrip any other transmission and access control protocol set.

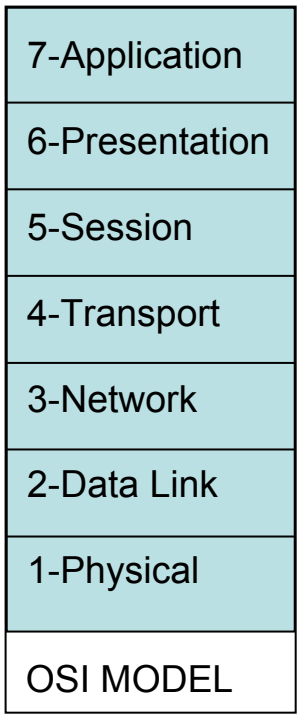
INDUSTRIAL NETWORKS AND BUSES

The range and types of industrial networks and buses are very broad as many evolved to handle specific types of industries and related applications. Some lay claim to more universality and interoperability. The focus will be on these network architectures since a prime pre-requisite for choosing a common network platform must include its ability to work with other networks and be standards-based. For convenience, the term network will be used to mean network or bus.

There are a number of ways to characterize the various networks, none that provide clear dividing lines, but for our purposes they will be grouped into *proprietary* and *open standard*. Even proprietary systems may provide gateway solutions for interconnectivity, but they require more configuration, modification, and testing than an open standard system. In addition, some networks attempt to standardize on the application and message syntax, or upper layers in Open System Interconnect (OSI) terminology. To keep things relatively simple, this paper addresses the lower layers responsible for getting the data to a destination device, user, or application.

Distributed with permission of author by ISA 2006
Presented at ISA EXPO 2006

If you've never seen the OSI model, avert your eyes from the following diagram. Too late. It's not possible to read any book on data communications and networking and avoid seeing this conceptual view of a generic network architecture. Fortunately, we will spend most of our time in layers one and two, which is where Ethernet operates.



To clarify terms, the physical layer deals with the transmission and synchronism of data and physical interface definition.

Layer two deals with the sending and receiving of data, validity of the data and retransmission, and access to the data link among other functions.

Layer three deals with network addresses, one example being an IP address, assembly and disassembly of messages, message sequencing, and routing.

Layer four deals with end-to-end exchange of messages.

The upper layers five to seven support the application and are beyond the scope of this paper. You can now breathe a sigh of relief.

PROPRIETARY NETWORKS

The following networks provide their own proprietary layer one and two implementations, but some offer alternate access via an Ethernet interface. In some cases the media may also be unique to the network. Some define an architecture using layer concepts similar to the OSI model above.

CANopen is a proprietary system using speed below 1 Mbit/sec and a line topology with drops. The CIA (Can-in-Automation) international user and manufacturer group provides standardization.

CC-Link is a Fieldbus network developed by Mitsubishi for real-time applications and is popular in Asia. It uses a line topology with speeds up to 10Mbit/s.

ControlNet was developed by Rockwell Automation and is a Fieldbus using line, bus, tree, and star topologies at 5Mbit/s.

DeviceNet, also developed by Rockwell Automation, operates at speeds up to 500 Kbit/s using a bus line with trunkline/dropline topology.

Interbus was developed by Phoenix Contact and is popular in automobile production. It operates at speeds up to 2Mbit/s using a ring topology with a unique cable design.

Modbus-IDA has three implementations, one using Token Bus at 2Mbit/s, another using a line topology, and a third version running over Ethernet/TCP/IP is discussed later.

Profibus is supported by Siemens and has a large presence in Europe with three protocol variations. It supports various media and topologies at speeds up to 12Mbit/s. The PROFINET spin-off is discussed later.

Foundation Fieldbus is a special case that straddles proprietary and open standards. It uses OSI terminology to define its architecture and offers a wide range of topology and speed variations in its H1 definition, and uses high speed Ethernet (HSE) for its H2 definition. Using layer concepts permits a greater chance of integration because of the defined boundaries.

SUMMARY

Lower speeds and a variety of topologies characterize these networks, but Profibus, Modbus, and Foundation Fieldbus have also joined the Ethernet bandwagon. While each network is important in its own right, none can claim its physical and data link layer protocols are good interconnect strategies, and thus need some type of gateway to communicate with other industrial networks. Next up, a review of the most important open standard networks.

OPEN STANDARD

The following networks were either created to be Ethernet-based, or evolved to support Ethernet and some TCP/IP functionality.

Industrial Ethernet Protocol (Ethernet/IP) was developed by Rockwell. As the name suggests it supports Ethernet and TCP/IP. Ethernet/IP supports line, star, and tree topologies at speeds of 10Mbit/s to 1 Gbit/s.

EtherCAT was developed by Beckoff and uses a switched Ethernet protocol at 100Mbit/s over line, star, tree, and ring topologies.

FL-net (OPCN-2) is supported by JEMA (Japan Electrical Manufacturers Association) and operates at speeds of 10Mbit/s and 100Mbit/s

Modbus-IDA Ethernet TCP/IP is an implementation of Rockwell's Modbus network that operates over Ethernet and TCP/IP. It operates at speeds of 10Mbit/s to 1 Gbit/s over star, tree, and line topologies.

Ethernet Powerlink was developed by B&R and supports TCP and UDP interfaces and runs at speeds of 10Mbit/s to 1 Gbit/s over star, bus, tree, and line topologies.

PROFINET runs over Ethernet and uses TCP for non-real-time applications at 100 Mbit/s over star, bus, tree, and line topologies.

SUMMARY

The open standard networks support multiple topologies over Ethernet at speeds of 100Mbit/s or better and provide TCP and UDP interfaces. This should make clear the evolution to high speed Ethernet over a variety of topologies.

INDUSTRIAL ETHERNET

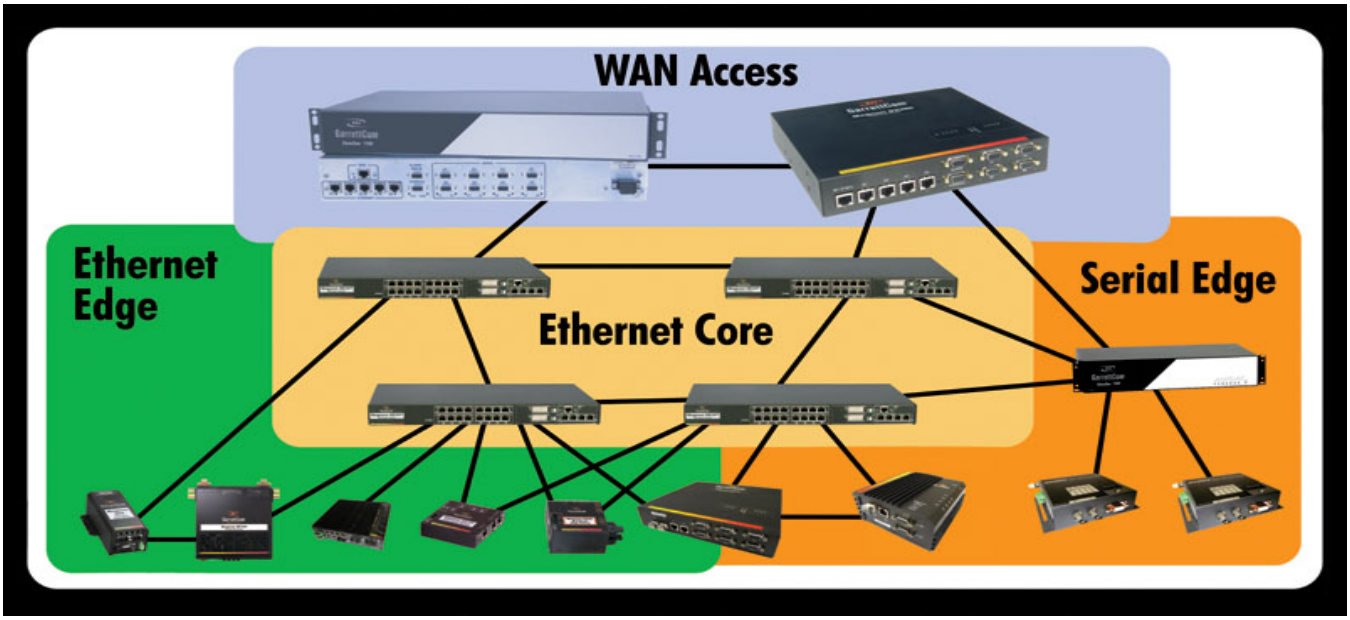
Industrial Ethernet supports the integration of existing sub-networks into a homogeneous network that includes effective routing, redundant links, and beefed up security. Many Ethernet vendors offer products designed for industrial environments. Ethernet hubs, managed and un-managed switches, media converters, and edge switches, hardened for hostile environments, are available at speeds up to the Gigabit range and operational over a variety of topologies using coax, copper, and fiber. Since many industrial networks already support Ethernet, integration is often straightforward.

Software is usually GUI-based to more effectively manage, configure, and monitor industrial networks. Ethernet managed and un-managed switches, including edge switches, coupled with the right topology provide the best solution to the control and support of remote sites such as power sub-stations and unattended sites.

Industrial Ethernet networking has inherent advantages. By utilizing a standards-based solution that supports multi-vendor implementations, industrial Ethernet users enjoy highly reliable systems with rapid recovery, reduced costs of deployment, and a guaranteed upgrade strategy as needs evolve. Redundancy and self-healing Ethernet networks provide the desired 24/7 uptime.

One other advantage of Ethernet is Power over Ethernet (PoE), which can greatly simplify the wiring of the many sensors, monitors, and input devices found in industrial Ethernet environments.

The illustration below depicts an integrated substation network which interconnects substations and central operations systems. Numerous Intelligent Electronic Devices (IEDs) such as relays, sensors, meters and Remote Terminal Units (RTUs), as well as surveillance cameras, VOIP phones and other devices are connected in a substation Local Area Network (LAN). Serial protocol devices are connected via routers or terminal servers, and Ethernet devices, including Power-over-Ethernet-enabled video cameras, are directly connected to Ethernet switches. The substation LAN connects to a Wide Area Network (WAN) router to transmit data to central operations systems and centers for processing and storage.



Integrated Substation Network

NETWORK INTEGRATION

The hard choices of integration include decisions of how to connect to proprietary systems. This will vary from industry to industry. Most legacy systems that continue to perform well are candidates for some form of gateway interface unless local management elements are fully effective or isolation from other networks is desirable. The security features of many Ethernet switches can block intrusions, and most routers offer firewalls and filtering options to keep systems secure.

When an older proprietary system is not performing, migration to Ethernet will permit a number of enhancements.

- Speed: A glance at the proprietary networks above indicate most are slower than 10Mbit/s. Ethernet ranges from 10Mbit/s to the Gigabit region and provides a huge bandwidth gain.
- Topology: The older systems often have an inflexible topology. Ethernet works with bus, star, mesh, and ring topologies.
- Nodes per net: Addressing schemes often limit the number of nodes. Slower speeds also limit the practical upper limit. The only limit in Ethernet is the bandwidth available.
- Redundant links: Ethernet has operated with redundancy for many years in enterprise systems that cannot afford downtime. Redundant link support is available for most topologies with a careful choice of Ethernet components.
- Standards-based: The flexibility of off-the-shelf components and the continual enhancements of Ethernet make solutions much easier to implement.
- Security: A wealth of security features is available. Managed switches have evolved into sophisticated components with many security features.

Distributed with permission of author by ISA 2006
Presented at ISA EXPO 2006

- Integration: The ability to manage a large network from central or distributed locations, economies of scale, network visibility, and other factors without time-consuming testing of incompatible interfaces can provide huge benefits.
- VLAN support: The ability to define virtual networks for managing traffic and security.

GATEWAYS

Gateways make communications possible between dissimilar systems. The range and types of gateway devices are broad, and the configuration and proper matching of two different interfaces can be a daunting task. The difficulty is based on how many layers of the two architectures must be matched and integrated. The ideal is to make the gateway transparent to both systems. System A thinks it is just talking to another member of its network and is not aware that system B is different.

When a gateway only has to deal with the routing, addressing, and transmission of data, the configuration is relatively simple. Referring back to the OSI model, this covers layers one to three. When it involves applications and message syntax, things get a lot stickier, and more time consuming. Also, the more layers that must be converted, the more processing overhead is involved. This can be unfortunate for critical real-time systems.

When the conversion involves the interconnection of systems and the transport of data, several Ethernet vendors offer components to efficiently handle that task.

- Media converters operate at the physical layer, match the signal transmission and media connecter differences. The data itself is transparent. Many Ethernet hubs and switches provide plug-in modules to simplify integration.
- Bridge devices generally operate at the data link layer (L2) and check L2 addresses, limiting unnecessary traffic. These can also be plug-in modules. Other so-called bridges operate more like routers and offer protocol conversion as well.
- Routers are layer three devices. Some provide protocol conversion using plug-in cards to handle token bus, token ring, and Ethernet protocols among others. A router checks L2 and L3 addresses and makes routing decisions based on its configuration. Others may offer support for proprietary protocols or a programming language to “roll your own” changes.

The amount of effort this takes, of course, is based on how dissimilar the systems are and how much control of the subnets is required. On the other hand, when everything is Ethernet-based and uses TCP/IP to support applications, the time, effort, and problems encountered are exponentially less.

USING ETHERNET TO NETWORK

There are many ways Ethernet components and standards can be employed to provide redundancy, robustness, security, and flexibility of design for many industrial networks. As has already been mentioned, Ethernet is also the best integration strategy available to network planners and architects.

TOPOLOGY AND REDUNDANCY

Ethernet works with star, bus, mesh, and ring topologies insuring the right topology for the job is selected. At the edges of a network with geographically separated devices the ring topology supported by Ethernet managed switches provides several advantages. Ethernet switches that support IEEE 802.1w, the Rapid Spanning Tree Protocol (RSTP), provide redundant links that can quickly recover from topology changes and add to the reliability of the ring. Because RSTP is designed to work with all topologies, some vendors offer proprietary and/or standards-based redundancy protocols that can significantly reduce recovery time down to as little as 50ms in the simple rings that are often used at the edge of a network.

Since the ring is comprised of devices with point-to-point links, signal reshaping and re-transmission of the sending leg reduce the possibility of transmission errors. Cabling costs are also significantly reduced from installing a separate link to each remote device as in a star or mesh topology. Where all devices are co-located a simple star or bus topology can be employed.

Some Ethernet switches support dual-homing. In Ethernet LANs, dual-homing is a network topology that adds reliability by allowing a device to be connected to the network by way of two independent connection points (points of attachment). One connection point is the operating connection, and the other is a standby or back-up connection that is activated in the event of a failure of the operating connection.

All media types from coax and copper to fiber are supported by Ethernet, often as plug-in modules for hubs and switches. Bandwidth to the Gigabit range is available in several combinations.

SECURITY

The 2003 Slammer worm attack on portions of the Northeast U.S. power grid confirmed the need for better security than currently implemented. The Energy Policy Act of 2005, which goes into effect the summer of 2006, provided a further push for a higher level of security in power systems. Both Ethernet and TCP/IP provide several sophisticated security features honed in IT departments and equally available to industrial Ethernet users.

Several TCP/IP-based and IEEE-based standards have been updated or created to handle intrusions over Internet-like connections. These include various forms of user authentication, password protection, and encryption. Managing a remote Ethernet component (switch, router, and hub) is most effective using standard GUI-based protocols. These in turn are translated into a command line

interface (CLI) sent to the target component. Using the Secure Socket Layer (SSL) protocol over HTTPS connections provides the same level of security enjoyed by Web-based financial transactions.

Simple Network Management Protocol version 3 (SNMPv3) limits access to sensitive Ethernet switches that feature SNMPv3 agent software/firmware. Data and operational control functions require user authentication, with access only permitted by specific IP addresses. Each IP address is configured during initial set-up.

The User-based Security Model (USM) of the SNMPv3 standard specifies the use of the Data Encryption Standard (DES-CBC), using a 56-bit key. Each manager must know the privacy key of each agent with which it communicates. Any Ethernet switches employed should provide remote access security for Telnet (CLI) communication, SNMP management, and Web-interface access.

Ethernet, because of its high bandwidth, is also the best protocol for deploying physical security devices at remote and peripheral sites. Power over Ethernet (PoE) adds ease of supplying power to remote security devices.

VIRTUAL LAN (VLAN) SUPPORT

VLANs are widely used today for reducing broadcast traffic by limiting the size of a collision domain. Since crossing a collision domain involves a routing decision, the security of a given domain can be assured. A VLAN creates separate collision domains or network segments that can span multiple Ethernet switches. A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. The IEEE 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

VLANs provide the capability of defining two or more Ethernet segments that co-exist on common hardware. The reason for creating multiple segments in Ethernet is to isolate collision domains. A collision domain includes all the cabling and hubs or repeaters supporting attached users, but excluding bridges or routers. Reducing the number of users per collision domain also reduces the chance of a collision and its recovery. VLANs can isolate groups of users, or divide up traffic for security or bandwidth management. VLANs need not be in one physical location; they can be spread across geography or topology.

VLANs, as the name suggests, create virtual LANs administratively. Instead of going to the wiring closet to move a cable to a different LAN segment, the same task can be accomplished remotely by configuring a port on an 802.1Q-compliant switch to belong to a different VLAN. The ability to move end stations to different broadcast domains by setting membership profiles for each port on centrally managed switches is one of the main advantages of 802.1Q VLANs.

SUMMARY ON BUS STRATEGIES

There are two reasons to maintain proprietary buses: legacy systems that are still providing satisfactory service, and highly tuned and specific applications. However, in a world where costs, high availability, and future-proofing are key operational objectives, industrial Ethernet is the clear winner for new deployments.

Industrial Ethernet provides the best support, redundancy, security, integration, and migration for industrial sites as they continue to evolve in the post-9/11 era. Specially hardened switches, hubs, and media converters provide reliable standards-based solutions to many industrial environments. Even sites with proprietary field buses and control buses can benefit by having Ethernet interfaces that provide a secure and redundant path to control centers and monitoring sites.

VLANs, SNMPv3 support, encryption, and SSL connections provide a secure environment as networks grow and adjust to an ever changing world.

BIBLIOGRAPHY

IEEE 802.1d and IEEE 802.1w Standards

Networking as a 2nd Language; Understanding Spanning Tree Protocol -- the Fundamental Bridging Algorithm, Michael Norton, O'Reilly Network, 03/30/01

Achieving Fault-Tolerance with PC-Based Control, David W. Cawlfield, ISA Automation & Control Subsystems Committee

IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1q-rev (D4) 2005

"Field Buses", http://www.interfacebus.com/Design_Connector_Field_Buses.html

"Redundancy with Standards in Industrial Ethernet LANs", Frank Madren, RTC Magazine, October 2003, http://www.rtcmagazine.com/home/article.php?id=100156

"What's Your Taste in Ethernet?" Wayne Labs, Contributing Editor, Control Design, June 26, 2005, http://www.controldesign.com/articles/2005/269.html

"Get going with Gigabit", Paula Doyle, Control Design March 23, 2006, http://www.controldesign.com/articles/2006/043.html

"Security in Industrial Applications", Frank Madren, Control Design, March 16, 2006, http://www.controldesign.com/whitepapers/2006/012.html

"Power over Ethernet (PoE) Makes Progress", Editorial, Control Design, March 16, 2006, http://www.controldesign.com/industrynews/2006/022.htm